Middle East Technical University

Department: Computer Science and Engineering

Year: Fall 2024-2025

Course: Discrete Computational Structures

Student's Solution

Name Surname: <Abdullah Burkan Bereketoglu> **Student ID:** <2355170>

1 Question 1 - Sets

1. **Proof of symmetric difference operation $\oplus$ is associative.**

$$A \oplus (B \oplus C) = (A \oplus B) \oplus C$$

where $A \oplus B = (A - B) \cup (B - A)$.

Q1.1

Step 1: Solve LHS $A \oplus (B \oplus C)$

$$\begin{aligned} B \oplus C &= (B - C) \cup (C - B) \\ A \oplus (B \oplus C) &= (A - ((B - C) \cup (C - B))) \cup (((B - C) \cup (C - B)) - A) \\ &= (A - B - C) \cup (B - C - A) \cup (C - A - B) \end{aligned}$$

After the distribution of the terms, we end up with similar terms as given below. Such similarities are eliminated hence for each value we get differences concerning other terms on the left-hand side.

$$A - B - C = A - C - B \quad \text{and similarly for other terms.}$$

Step 2: Solve RHS $(A \oplus B) \oplus C$

$$\begin{aligned} A \oplus B &= (A - B) \cup (B - A) \\ (A \oplus B) \oplus C &= ((A - B) \cup (B - A)) \oplus C \\ &= (A - B - C) \cup (B - A - C) \cup (C - A - B) \end{aligned}$$

Deduction/To Conclude: As can be seen both sides ($A\oplus(B\oplus C)$ and $(A\oplus B)\oplus C$) give the difference of sets concerning other sets in the system, hence; are equal so the associativeness is shown.

$$A \oplus (B \oplus C) = (A \oplus B) \oplus C$$

Therefore, the symmetric difference operation $\oplus$ is associative.

2. ## Q1.2

Prove that g is one-to-one.

Proof

To show that g is one-to-one, we need to prove that for any $a_1, a_2 \in A$, if $g(a_1) = g(a_2)$, then $a_1 = a_2$.

1. Assume for some $a_1, a_2 \in A$, put them in f and assume $g(a_1) = g(a_2)$
2. For $f(a_1) = f(a_2)$, since f is 1-to-1 this implies $a_1 = a_2$.
3. Also $f \circ g$ is 1-to-1, so take $a_1, a_2 \in A$ for

$$f(g(a_1)) = f(g(a_2))$$

4. This implies $(f \circ g)(a_1) = (f \circ g)(a_2)$ also we found that $a_1 = a_2$.
5. Hence, $g(a_1) = g(a_2)$ implies $a_1 = a_2$, which proves that g is one-to-one , QED.

3. ## Q1.3

Since in question it is asked from us that we use the contradictory assumption ($f : S \to \mathcal{P}(S)$ is onto), we will do so, and define a set that is described in the question as T.

Subset of T can be defined as $T = \{s \in S \mid s \notin f(s)\}$ and it consists of all elements in S that are not in the image under f.

Hence, we will show if an element is in $s_T \in S$ also satisfies the condition of $f(s_T) = T$.

1. For $s_T \in T$, then by our definition of T, $s_T \notin f(s_T)$, that indicates $s_T \notin T$ (a contradiction of the definition of T).
2. For $s_T \notin T$, then by our definition of T, $s_T \in f(s_T)$, that indicates $s_T \in T$ (a contradiction which is the opposite case of prior one).

For all cases $f(s_T) = T$ assumption leads to a contradiction. This means s_T can't be both in T and not be simultaneously. This contradiction shows no possible satisfactory s_T and means initial assumption f being onto is false and cannot exist.

4. **Q1.4**

(a) **Is** $f(m,n) = 2m + n$ **onto?**

To prove if the function is onto, show it spans the co-domain from its domain which is $Z \times Z \implies Z$. Therefore, let $n = -m$ for any $m \in \mathbb{Z}$:

$$f(m,n) = 2m + (-m) = m.$$

Since m m can be any integer so as n, hence; we can obtain all integers by choosing n as such: $n = -m$ for any m. Moreover, we can also state this for any arbitrary integer k, $m = k$ and $n = -k$

(b) **Is** $f(m,n) = m^2 - n^2$ **onto?**

Factor it as:

$$f(m,n) = m^2 - n^2 = (m+n)(m-n).$$

Here we will show it is not **onto** by a contradiction. such as $f(m,n) = 2$:

- If $m + n = 2$ and $m - n = 1$, or $m + n = 1$ and $m - n = 2$ there are no integer solutions for such m and n.

This shows not all values of Z co-domain can be generated, hence **not onto**.

(c) **Is** $f(m,n) = m + n + 1$ **onto?**

Consider any integer k:

$$k = m + n + 1.$$

When we rearrange the function as $m + n = k - 1$. By choosing $m = k - n - 1$ and $n \in Z$, we get:

$$f(m,n) = (k - n - 1) + n + 1 = k.$$

Since, n spans the Z both in domain and co-domain, therefore; m spans also. and equals an odd value with no coefficient which indicates $k \in Z$. Hence it is onto.

(d) **Is** $f(m,n) = |m| - |n|$ **onto?**

Function outputs to co-domain Z by m and n as absolute value difference. It's property to any $k \in \mathbb{Z}$, which means onto.

- If $|m| \geq |n|$, then $f(m,n) \geq 0$.
- If $|n| \geq |m|$, then $f(m,n) \leq 0$.

By adjusting $|m|$ and $|n|$, we can achieve any integer $k \in \mathbb{Z}$:

- To produce any $\mathbb{Z}^+$ for$k$, set $|m| = k + |n|$.
- To produce any $\mathbb{Z}^-$ for $-k$, set $|n| = k + |m|$.
- and to include 0, set $|m| = |n|$.

Hence we achieved, $\mathbb{Z}^+ \cup \mathbb{Z}^- \cup 0$. Which means **onto** to $\mathbb{Z}$.

(e) **Is** $f(m,n) = m^2 - 4$ **onto?**

Again as part b of the question by a contradicting example, we can show this function is not onto in $\mathbb{Z}$.

For this to be onto, any integer $k \in \mathbb{Z}$ should be mapped from $m^2 - 4$. Rearranging gives:

$$m^2 = k + 4.$$

For m to be an integer, $k + 4$ must be bigger or equal to 0, and needs to be a square value. However, for not all integers $k \in \mathbb{Z}$ it is positive. For example, $k = -5$ gives $m^2 = -1$, which leads to $m = i$ hence not in $\mathbb{Z}$.

Which means the function is **not onto**.

Q1.5

5. (a) Solve:

$$\bigcap_{i=2}^{\infty} \left(0 - \frac{1}{i}, 5 + \frac{1}{i}\right).$$

Each finite interval $\left(0 - \frac{1}{i}, 5 + \frac{1}{i}\right)$ is open, but includes points slightly below 0 and above 5 for any i that is again finite. As $i \to \infty$, then the endpoints approach to 0 and 5.

$$\bigcap_{i=2}^{\infty} \left(0 - \frac{1}{i}, 5 + \frac{1}{i}\right) = [0, 5].$$

In the end, as intersections of infinite sets with open boundaries, end up being closed sets, if the bounds are inside for each finite intersection, such as this example.

Hence, when taking the intersection of infinitely many open intervals that are bigger and including the 0 and 5, will converge to $[0, 5]$, therefore at the **final set we include 0 and 5**. The limiting case is closed interval $[0, 5]$, where 0 and 5 are included where we **never excluded 0 and 5**. Never eliminated.

(b) Solve:

$$\bigcup_{i=2}^{\infty} \left[0 + \frac{1}{i}, 5 - \frac{1}{i}\right].$$

Each finite interval $\left[0 + \frac{1}{i}, 5 - \frac{1}{i}\right]$ is closed, even though has close values to 0 and 5, they do not exactly include values 0 and 5. As $i \to \infty$, then the left-hand and right-hand boundaries/endpoints reach to 0 and 5, but never finitely include them. Then the final set can be written as;

$$\bigcup_{i=2}^{\infty} \left[0 + \frac{1}{i}, 5 - \frac{1}{i}\right] = (0, 5).$$

Unin of infinitely many closed sets that **never include borders in finite region** and $(0, 5)$ as $i \to \infty$, we then deduce that 0 and 5 are **never included** as in the final set. Thus the corresponding set is an open set as $(0, 5)$, and not including the 0 and 5, and never included/added

2 Question 2 - Algorithms

1. To determine if $\sin x = O(\cos x)$, we need to provide some witnesses as $c > 0$, $x_0 \geq 0$ and $x \geq x_0$ where x_0 can be considered as k, if there exists a start of the bound.

$$|\sin x| \leq c|\cos x|.$$

For the general case of $\sin x$ and $\cos x$, both $\sin x$ and $\cos x$ oscillate between -1 and 1 indefinitely as $x \to \infty$. Therefore, there is no constant c that satisfies $|\sin x| \leq c|\cos x|$ for all x. Hence, no constant c $\sin x$ is not $O(\cos x)$.

2. **Answer Q2.2:**

Assume $f(x) = O(x)$, for this assumption, we want to find the implication of $f(x) = O(x^2(2+\cos x))$, for $f(x) = O(x)$ there exist constants $c_1 > 0$ and $x_1 \geq 0$ such that $\forall x \geq x_1$,

$$|f(x)| \leq c_1|x|.$$

Let $g(x) = x^2(2 + \cos x)$. Here the $2 + \cos x$ oscillates between 1 and 3, so $g(x)$ grows asymptotically as the term x^2.

Since $f(x) = O(x)$, $\exists c_2 > 0$ and $\forall x_2 \geq 0$ such that:

$$|f(x)| \leq c_2|x| \leq c_2 x^2(2 + \cos x), \quad \text{for } x \geq x_2.$$

As for some witnesses $x_1 \& x_2 = k_1 \& k_2$ and c, it is evident that x^2 grows faster than x, and the secondary part is shown not decreasing, but rather fluctuating with x^2 domination, we can deduce and proven that $f(x) = O(x^2(2 + \cos x))$ with appropriate choice of witnesses.

3. **Show that $x \log x$ is $O(x^2)$ but x^2 is not $O(x \log x)$.**

Answer Q2.3:

Q2.3.1: $x \log x = O(x^2)$

Here we are asked to show, $x \log x = O(x^2)$. With witnesses $c > 0$ and $x_0 \geq 0$ such that for all $x \geq x_0$, where the limiting case $x_0 = k$

$$x \log x \leq cx^2.$$

For large x, $\log x << x$, so $x \log x$ grows slower than x^2 since $x^2 \geq x * x$. Let $c = 1$. Then for $x \geq 1$,

$$\frac{x \log x}{x^2} = \frac{\log x}{x} \to 0 \quad \text{as } x \to \infty.$$

This limit shows that the equation provided is bounded by the provided big-O, hence; $x \log x = O(x^2)$.

Q2.3.2: Show x^2 is not $O(x \log x)$

To show x^2 is not bounded with $O(x \log x)$, assume for contradiction that there exist witnesses $c > 0$ and $x_0 \geq 0$ such that for all $x \geq x_0$,

$$x^2 \leq cx \log x.$$

By dividing both sides with x (for $x > 0$), we get:

$$x \leq c \log x.$$

As from Q2.3.1, we know that as $x \to \infty$, x grows faster than $\log x$, so there is no such witness c that satisfies this inequality for large, for all x. Thus, x^2 is not $O(x \log x)$.

As a result of both parts, $x \log x = O(x^2)$ however, x^2 is not $O(x \log x)$.

3 Question 3 - Divisibility

1. We use prove by contradiction and the hint of the Fundamental Theorem of Arithmetic (unique factorization theorem), showing as primes, hence;$\sqrt{7}$ is irrational.

    1. Assume, $\sqrt{7}$ is rational. Then we can write it as $\sqrt{7} = \frac{a}{b}$, where a and b are integers with $\gcd(a, b) = 1$, which means it is in it's simplest form.
    2. We take squares of both sides and get:
    $$7 = \frac{a^2}{b^2} \Rightarrow a^2 = 7b^2$$
    3. This equation implies that a^2 is divisible by 7, which means a must also be divisible by 7 since a, and b are integers and 7 is prime.
    4. Let $a = 7t$ for some integer t. Then substitute it to the equation, and get:
    $$(7k)^2 = 7b^2 \Rightarrow 49k^2 = 7b^2 \Rightarrow b^2 = 7k^2$$
    5. Now, 7 is on the other side meaning that as b is integer it must also be divisible by 7.
    6. Since both a and b are divisible by 7, this shows $\frac{a}{b}$ is not in it's simplest form, hence; leading to a contradiction. QED.

    Therefore, $\sqrt{7}$ is not rational, but irrational.

2. Here we prove by contradiction by assuming there are only finitely many primes of the form $3k + 2$. Let these primes be $q_1, q_2, \ldots, q_n$.

    1. Consider the number $N = 3q_1q_2 \cdots q_n + 2$.
    2. $N \equiv 2 \pmod 3$ as can be seen as;
    $$3q_1q_2 \cdots q_n \equiv 0 \pmod 3 \Rightarrow N = 3q_1q_2 \cdots q_n + 2 \equiv 2 \pmod 3$$
    3. Since $N \equiv 2 \pmod 3$, $3k + 1$ or 3 cannot satisfy this condition so, any prime factor of N must also be of the form $3k + 2$ or it should be prime.
    4. Also, N is not divisible by any of $q_1, q_2, \ldots, q_n$ since there exists a $+2$ for each there will always be a $+2$ remainder.
    5. Which leads to the statement of either N is a new prime of the form presented or has a prime factor not in the set which is not possible (it will be a contradiction.). Due to this contradiction, this leads that there exist infinitely many of primes of form $3k + 2$.

3. Given $a \equiv b \pmod m$, we have $m \mid (a - b)$ divisible by m, this indicates $a = b + cm$ for some arbitrary integer c. By this we can show with some steps the $\gcd(a, m) = \gcd(b, m)$ equality.

    1. Let for LHS $div = \gcd(b, m)$. Gives, $div \mid b$ and $div \mid m$.

2. Also, $a = b + cm$, which will give that for any divisor of b and m divides a.
3. Moreover, $div \mid a$ and $div \mid m$, so it indicates a common divisor of a and m which is div, implying $div \leq \gcd(a, m)$.
4. For RHS assume $div' = \gcd(a, m)$. Then $div' \mid a$ and $div' \mid m$, which means $div' \mid (a - km) = b$.
5. Again, as we did for LHS, same statements for RHSdiv' is a common divisor of b and m, so $div' \leq \gcd(b, m) = div$.
6. As a result we get, $d \leq d'$ and $d' \leq d$, hence $d = d'$, which means $\gcd(a, m) = \gcd(b, m)$.